Available online at www.sciencedirect.com
SCIENCE DIRECT®
PERGAMON
Chaos, Solitons and Fractals 18 (2003) 881–890
CHAOS SOLITONS & FRACTALS
www.elsevier.com/locate/chaos

Secure digital communication using discrete-time chaos synchronization

Moez Feki *, Bruno Robert, Guillaume Gelle, Maxime Colas

Université de Reims Champagne Ardenne, Moulin de la Housse BP 1039, 51687 Reims cedex 2, France

Accepted 21 February 2003

Abstract

In this paper we propose some secure digital communication schemes using discrete chaotic systems. In our approach a message is encrypted at the transmitter using chaotic modulation. Next, the driving signal synchronizes the receiver using discrete observer design or drive-response concept. Finally, by reverting the coding procedure the transmitted message is reconstructed. To demonstrate the efficiency of our communication schemes a modified Hénon's map is considered as an illustrative example.

1. Introduction

Chaotic synchronization of continuous-time as well as discrete-time chaotic systems has been the focus of a growing literature since the last decade [1–6]. This research is motivated in part by its potential application in secure communication [7–11]. Due to the sensitive dependence on initial conditions and the random-like behaviour of chaotic signals in addition to their broadband spectrum, it was believed that information could be hidden efficiently in chaos.

Actually, three main message encoding schemes were developed: chaotic masking [7], chaos shift keying [12] and chaos modulation [13]. In chaotic masking the message to be transmitted is added to a much stronger chaotic signal in order to hide the information, the overall signal is then transmitted to the receiver. In chaos shift keying the transmitted signal is obtained by switching between N chaotic generators according to the information level of an N-ary message (usually binary messages are used with two chaotic generators). In chaotic modulation the message modifies the state or the parameters of the chaotic generator through an invertible procedure, thus the generated chaotic signal inherently contains the information on the transmitted message.

Irrespective of which of the foregoing encoding schemes is used for message encryption, a duplicate of the transmitter's chaotic signal should be available at the receiver side in order to reconstruct the message. Or better yet, the receiver should synchronize with the transmitter. Attempts on chaos communication using analog systems [14,15], especially those which use masking scheme [16], revealed serious weakness since the message reconstruction overwhelmingly depends on the synchronization error, whence it can be easily corrupted by channel noise. Therefore, research towards using discrete chaotic systems was favoured. In [17], Parlitz and Ergezinger proposed a robust communication method using modulation by digital message, however, to synchronize the transmitter and the receiver both systems are supposed to start at the same time and from the same initial conditions which are unpractical conditions. In addition, the message is transmitted at low rate due to redundancy, in fact N chaotic samples are required to transmit one information sample. In [11] Liao and Huang suggested a modulation scheme by adding a discrete message to the chaotic output then the resulting signal is fed back into the transmitter system and at the same time it is sent to

* Corresponding author. Tel.: +33-3-26-91-85-79; fax: +33-3-26-91-31-06.
E-mail address: moez.feki@univ-reims.fr (M. Feki).

0960-0779/03/$ - see front matter
doi:10.1016/S0960-0779(03)00065-1

drive the receiver system. This scheme uses observer-based synchronization and avoids redundancy. However, though it is successful in some cases, it suffers from several drawbacks: First, only low power messages can be transmitted which makes the scheme very vulnerable to distorting channel noise. Second, the message feedback applied to certain chaotic systems such as Hénon's map may lead to divergence of the originally chaotic states.

Herein, we present two different schemes of message encoding based on chaotic modulation. In the first scheme, the binary message ($m(k) = \pm 1$) is multiplied by the output chaotic signal of the transmitter and then sent to drive the receiver system. To ensure the synchronization of the transmitter and the receiver systems, some hypotheses need to be satisfied. In the second scheme, the binary message is modulated by multiplication with the chaotic output signal then it is fed back to the transmitter system and simultaneously sent to the receiver system. In order to synchronize with the transmitter, a Luenberger-like discrete observer is used as a receiver. We show that under mild conditions dead-beat synchronization is achieved. Therefore, message reconstruction can simply be obtained by reverting the encoding procedure. Furthermore, no constraints on the message power is required, besides a simple modification of Hénon's map is suggested to remedy the problem of divergence due to feedback.

This paper is outlined as follows. In Section 2, chaotic synchronization using discrete observer is shown. Section 3 is devoted to present the communication schemes. In Section 4, we consider Hénon's map as an illustrative example, we show the influence of the modulated signal feedback on the transmitter system and we suggest a system modification as a remedy. In Section 5, results from numerical simulations are presented. Finally, in Section 6, we outline some concluding remarks and perspectives.

2. Observer-based discrete synchronization

Discrete-time chaotic systems are generally described by a set of nonlinear difference equations. It is very common, however, to be able to separate the dynamics into linear and nonlinear parts. If we furthermore consider that the chaotic system is a Lur'e type system then it can be described by the following equations:

$$x(k+1) = Ax(k) + f(y(k)) \tag{1a}$$

$$y(k) = Cx(k) \tag{1b}$$

where k is the discrete time, $x \in \mathbb{R}^n$ and $y \in \mathbb{R}$ are respectively the state vector and the output of the drive system. A and C are two constant matrices of appropriate dimensions and $f : \mathbb{R} \to \mathbb{R}^n$ is a real vector field.

We notice that Hénon's map and Lozi's piecewise linear model are two well known discrete-time chaotic systems that can be written in the form of (1).

As a response system, we consider the Luenberger-like discrete observer with $y(k)$ being the driving sequence

$$\hat{x}(k+1) = A\hat{x}(k) + f(y(k)) + L(y(k) - \hat{y}(k)) \tag{2a}$$

$$\hat{y}(k) = C\hat{x}(k) \tag{2b}$$

where $\hat{x}$ is the state vector of the response system and $L \in \mathbb{R}^n$ is an observer gain chosen to satisfy drive-response synchronization i.e., $\lim_{k\to\infty}(x(k) - \hat{x}(k)) = 0$.

Let's define a synchronization error $e(k) = x(k) - \hat{x}(k)$, consequently the error dynamics are

$$e(k+1) = (A - LC)e(k) = A_c e(k) \tag{3}$$

and the solution of (3) given an initial condition $e(0) = x(0) - \hat{x}(0)$ is

$$e(k) = A_c^k e(0) \tag{4}$$

Clearly if the pair (A, C) is observable then L can be chosen such that the spectral radius of A_c is less than 1. Therefore, (3) is stable and $\lim_{k\to\infty} e(k) = 0$. Moreover, if L is chosen such that A_c is a nilpotent matrix of order p i.e., $A_c^p = 0$ then the error will fade to zero after p steps thereby a finite time synchronization, denoted by dead-beat synchronization [18], is obtained regardless of the initial conditions.

3. Modulating chaos with digital message

In this section chaotic communication systems are suggested using the drive-response synchronization and observer-based synchronization. The drive system is used as a transmitter and the response system is the receiver. The driving chaotic sequence used for synchronization is modulated by a binary message, hence slight modification of the transmitter–receiver system is required to achieve synchronization.

3.1. Modulation by multiplication

In this scheme Lur'e type chaotic systems are used. The chaotic output sequence $y(k)$ is multiplied by the message sequence $m(k)$ which is binary coded and satisfy the following hypothesis:

($\mathscr{H}1$) The transmitted message is binary coded with (−1,+1) are the only admitted values.

The resultant modulated sequence $s(k) = y(k) \cdot m(k)$ is then sent to the receiver. Since $y(k)$ is not available at the receiver side, the feedback term $L(y(k) - \hat{y}(k))$ in (2a) cannot be implemented. Nevertheless, synchronization can be achieve if the following hypothesis is satisfied:

($\mathscr{H}2$) A is stable and the nonlinearity of the chaotic system is even.

Finally, we have the following communication system

$$\text{transmitter}\begin{cases} x(k+1) = Ax(k) + f(y(k)) \\ y(k) = Cx(k) \\ s(k) = y(k) \cdot m(k) \end{cases} \tag{5}$$

$$\text{receiver}\begin{cases} \hat{x}(k+1) = A\hat{x}(k) + f(s(k)) \\ \hat{y}(k) = C\hat{x}(k) \end{cases} \tag{6}$$

Using hypothesis ($\mathscr{H}2$), the subsequent synchronization error dynamics are described as follows

$$e(k+1) = Ae(k) + f(y(k)) - f(y(k) \cdot m(k)) = Ae(k),$$

thereby the synchronization error fades to zero exponentially fast. Hence, the message can be reconstructed in the following manner

$$\hat{m}(k) = \frac{s(k)}{\hat{y}(k)} = \frac{Cx(k)}{C\hat{x}(k)} \cdot m(k) \tag{7}$$

It is obvious that if $\hat{x}(k) = x(k)$ then $\hat{m}(k) = m(k)$.

3.2. Modulation by multiplication and feedback

In this scheme the chaotic output is multiplied by the message sequence and the obtained sequence is simultaneously sent to the receiver and fed back to the transmitter. In fact, this new scheme constitutes a new solution to synchronize the transmitter and the receiver without putting forward hypotheses ($\mathscr{H}1$) and ($\mathscr{H}2$). The communication system is described by the following equations, where $s(k)$ is the information bearing signal which drives the receiver

$$\text{transmitter}\begin{cases} x(k+1) = Ax(k) + f(s(k)) + L(s(k) - y(k)) \\ y(k) = Cx(k) \\ s(k) = y(k) \cdot m(k) \end{cases} \tag{8}$$

$$\text{receiver}\begin{cases} \hat{x}(k+1) = A\hat{x}(k) + f(s(k)) + L(s(k) - \hat{y}(k)) \\ \hat{y}(k) = C\hat{x}(k) \end{cases} \tag{9}$$

The ensuing synchronization error dynamics are described as follows

$$e(k+1) = Ae(k) + L(s(k) - y(k)) - L(s(k) - \hat{y}(k)) = A_c e(k)$$

thus if the pair (A, C) is observable then we can choose L such that A_c is nilpotent, thus dead-beat synchronization is achieved. However, if (A, C) is only detectable then we can choose L such that A_c is at least stable and the synchronization error fade to zero exponentially fast.

Eventually, message reconstruction is obtained by inverting the encoding procedure, that is

$$\hat{m}(k) = \frac{s(k)}{\hat{y}(k)} = \frac{Cx(k)}{C\hat{x}(k)} \cdot m(k) \tag{10}$$

It is obvious that if $\hat{x}(k) = x(k)$ then $\hat{m}(k) = m(k)$.

Remark 1. We note that if A is nilpotent or at least stable then the communication scheme is valid with the choice of $L = 0$. Let for example the following chaotic transmitter

$$x_1(k+1) = \sqrt{2}x_2(k), \quad x_2(k+1) = \sqrt{2}x_3(k), \quad x_3(k+1) = 1 - 0.5x_1(k)^2.$$

with

$$A = \begin{bmatrix} 0 & \sqrt{2} & 0 \\ 0 & 0 & \sqrt{2} \\ 0 & 0 & 0 \end{bmatrix} \quad f(x) = \begin{pmatrix} 0 \\ 0 \\ 1 - 0.5x_1(k)^2 \end{pmatrix}$$

It is easy to verify that $A^3 = 0$ and f is even.

4. Modifying Hénon's map for communication

In the foregoing section two communication schemes were presented. The first scheme concerns a restricted class of chaotic systems. However, the second scheme seems to concern a larger class of systems. Nevertheless, further analysis needs to be carried to investigate the effect of $s(k)$ feedback on the chaotic behaviour of the transmitter. To ease the analysis, the chaotic system considered in this paper is the well known Hénon's map.

$$x_1(k+1) = 1 - 1.4x_1(k)^2 + x_2(k) \tag{11a}$$

$$x_2(k+1) = 0.3x_1(k) \tag{11b}$$

By choosing $y(k) = x_1(k)$, it can be seen that (11) is in the form of (1) with

$$A = \begin{bmatrix} 0 & 1 \\ 0.3 & 0 \end{bmatrix} \quad \text{and} \quad f(x) = \begin{pmatrix} 1 - 1.4x^2 \\ 0 \end{pmatrix}$$

Obviously A is stable and f is an even function and the first scheme of the previous section can be applied to Hénon's map.

On the other hand, if the second scheme is applied, with $L = (0, 0.05)^{\mathrm{T}}$ chosen such that A_c is stable, the transmitter is described as follows

$$x_1(k+1) = 1 - 1.4s(k)^2 + x_2(k) \tag{12a}$$

$$x_2(k+1) = 0.3x_1(k) + 0.05x_1(k)(m(k) - 1) \tag{12b}$$

$$s(k) = x_1(k) \cdot m(k) \tag{12c}$$

Since f is even the $f(s(k)) = f(x(k))$ and (12) can be rewritten in compact form

$$x(k+1) = \begin{cases} A_{(-1)}x + f(x) & \text{if } m(k) = -1 \\ A_{(+1)}x + f(x) & \text{if } m(k) = +1 \end{cases} \tag{13}$$

where

$$A_{(-1)} = \begin{bmatrix} 0 & 1 \\ 0.2 & 0 \end{bmatrix} \quad A_{(+1)} = \begin{bmatrix} 0 & 1 \\ 0.3 & 0 \end{bmatrix}$$

Note that we have obtained parameter modulation which is very close to chaos shift keying. Besides the two Henon's maps described in (13), henceforth denoted by $H_{(-1)}$ and $H_{(+1)}$, have different attractors and different basins of attraction that we denote $B_{(-1)}$ and $B_{(+1)}$. Let k_0 be the discrete time at which the state $x(k_0) \in B_{(+1)}$ and $x(k_0) \notin B_{(-1)}$. Suppose that $m(k) = -1$, $k = k_0 + 1, \ldots, k_0 + i$, $i > 0$ then $x(k)$ will diverge. If the state gets out of $B_{(+1)}$ then $x(k_0 + i) \notin \{B_{(-1)} \cup B_{(+1)}\}$. Therefore, the behaviour of the transmitter becomes divergent and not chaotic.

Should the intersection of the basins of attraction contain both attractors then the transmitter keeps having a chaotic behaviour if the state is initiated inside the intersection $x(0) \in \{B_{(-1)} \cap B_{(+1)}\}$. Therefore, our goal is to modify Henon's map to extend the basin of attraction to $\mathbb{R}^2$, thereby the intersection condition is satisfied. From (11), the dynamics of Henon's map can be separated into linear and nonlinear parts. Since the map is chaotic then it is locally expanding.

Let's suppose that $f(x(k))$ is a feedback control to a linear system and let it be denoted by $f(x(k)) = Bu(k)$. Hence we can write

$$x(k+1) = Ax(k) + Bu(k)$$

Let $x_1(k)$ be the output and $H(k)$ be the impulse response of the linear system, then we have

$$x_1(k) = \sum_{j=0}^{k} u(k-j)H(j)$$

Now since A is stable it follows that $H(k)$ is a decaying function, thus there exists positive constants $M > 0$ and $1 > \sigma > 0$ such that

$$|H(k)| < M|\sigma|^k$$

Note that $u(k) = f_1(x_1(k)) = 1 - 1.4x_1(k)^2$, so if $x_1(k) \in [-1.2746, 1.2746]$ then $u(k) \in [-1.2746, 1.2746]$ and

$$x_1(k) < 1.275 \sum_{j=0}^{k} |H(j)| < 1.275 \frac{M}{1-|\sigma|}$$

However, if $x_1(k) \notin [-1.2746, 1.2746]$ then $|u(k)| > |x_1(k)|$, therefore we intuitively expect that each future iteration is excited by a larger input and hence $x_1(k)$ may diverge. For more rigorous analysis on the behaviour of Henon's map we refer the reader to [19].

To avoid divergence, it is sufficient to make $u(k)$ bounded for all values of $x_1(k)$. Let $\tilde{f}_1(x(k))$ be periodic of period $2P$ and defined by

$$\tilde{f}_1(x_1(k)) = 1 - 1.4\left(x_1(k) - \text{floor}\left(\frac{x_1(k)+P}{2P}\right)2P\right)^2$$

where floor(a) rounds a to the nearest integer towards minus infinity. It is clear that for $x_1(k) \in [-P, P]$ we have $\tilde{f}_1(x_1(k)) = f_1(x_1(k))$. Now since $\tilde{f}_1(x_1(k))$ is periodic then for a suitable choice of $P = 1.2746$ we have $u(k) \in [-1.2746, 1.2746]$ for all values of $x_1(k)$ whence

$$x_1(k) < 1.275 \frac{M}{1-|\sigma|}$$

Eventually, the modified Henon's map becomes locally expanding and globally bounded.

5. Simulation results and analysis

5.1. Modulation by multiplication

Using Henon's map presented in (11), we have simulated the communication scheme using modulation by multiplication. It is clear that A is stable with eigenvalues $\lambda = \pm 0.5477$, therefore the synchronization is achieved exponentially fast. Fig. 1 shows the simulation results. The output chaotic signal $x_1(k)$ and the message $m(k)$ are superposed in Fig. 1a and their multiplication yields $s(k)$ shown in Fig. 1b. The recovered message and the error $e_m(k) = m(k) - \hat{m}(k)$ are presented in Fig. 1c and d. It is clear that the reconstruction is correct except for the first sample where the synchronization error is still significant. To improve the performance of this communication scheme, the choice of the chaotic transmitter is crucial. Indeed, if the chaotic system has a linear part with a nilpotent matrix then the synchronization is achieved in finite time.

5.2. Modulation by multiplication and feedback

We have seen in the foregoing section that this scheme yields to parameter modulation and hence two Henon's maps were obtained. Fig. 2 sketches the attractors of $H_{(+1)}$ and $H_{(-1)}$. Fig. 3 depicts an example of a message that yields to divergence of this scheme if Henon's map is used (note that $s(k) \approx 10^{154}$). As it has been elucidated in Section 4, and without loss of generality we considered in this example $k_0 = 0$, $x(0)$ is sketched by an asterisk in Fig. 2 and it is in the vicinity of the attractor of $H_{(+1)}$. $x(0) \in B_{(+1)}$ but $x(0) \notin B_{(-1)}$. Therefore, with $m(k) = -1$, $k = 1, 2, 3$, it is shown by simulation that $x(k)$ diverges and leave the chaotic orbits. Although, the message is numerically recovered, the communication scheme is unsuccessful.

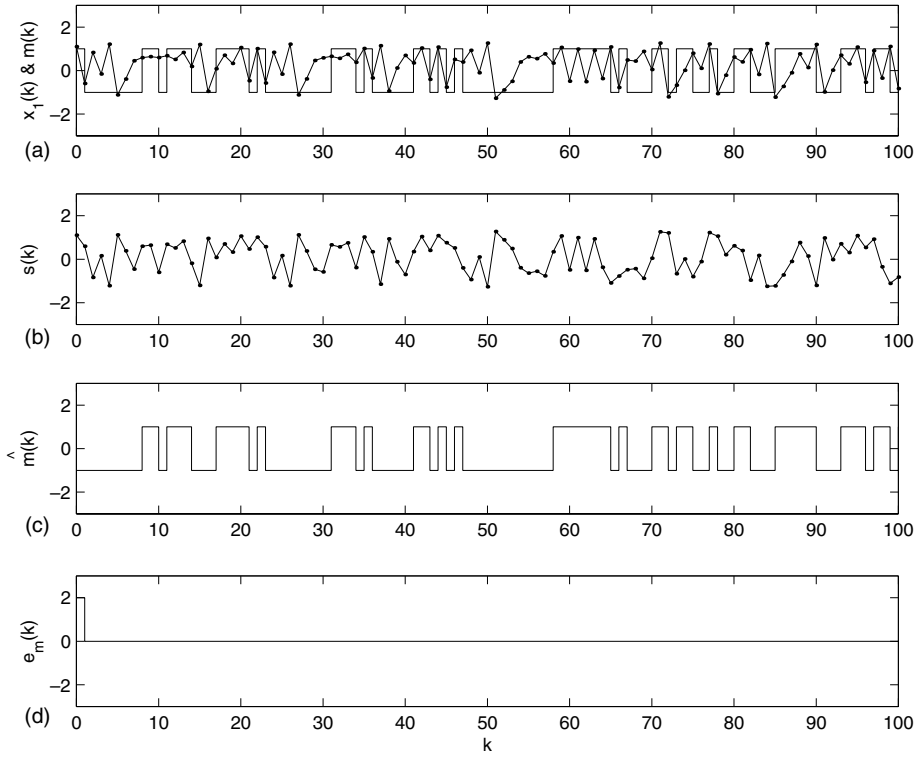

Fig. 1. Transmission using modulation by multiplication.

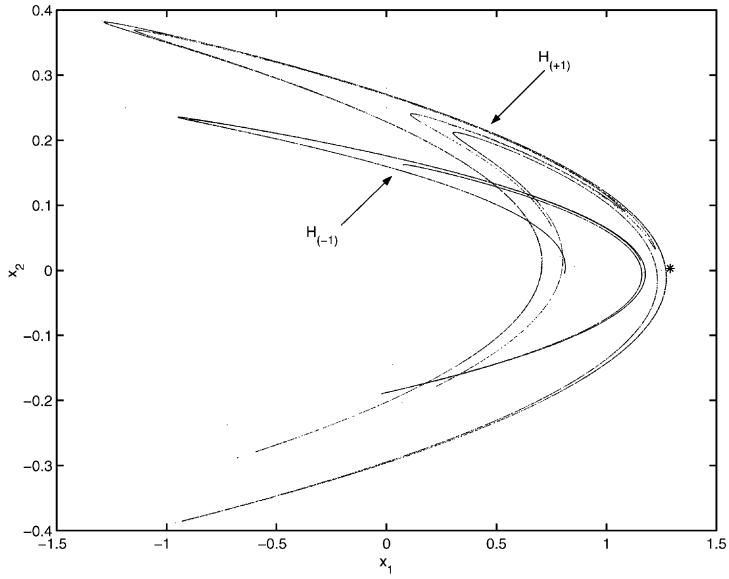

Fig. 2. Attractors of $H_{(+1)}$ and $H_{(-1)}$.

The modification proposed, was to substitute $f_1(x_1(k))$ by $\tilde{f}_1(x_1(k))$, both functions are sketched in Fig. 4. Since $\tilde{f}_1(x_1(k))$ folds $\mathbb{R}$ into the interval [−1.2746,1.2746], the basin of attraction of the modified Hénon's map extends to $\mathbb{R}^2$

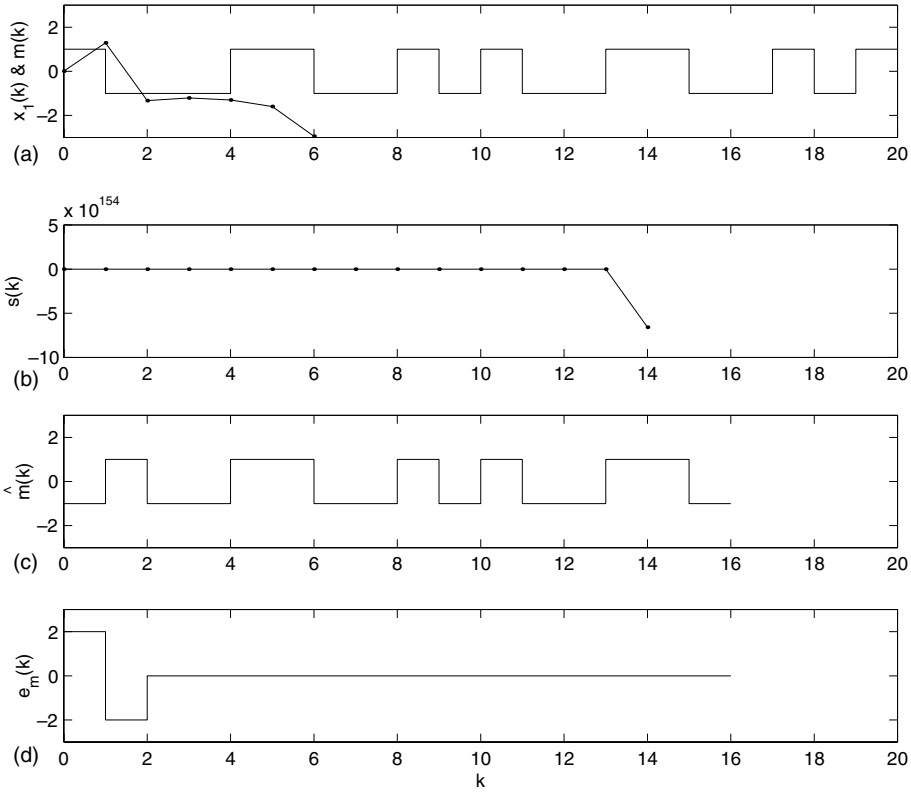

Fig. 3. An example of modulation failure using Hénon's map.

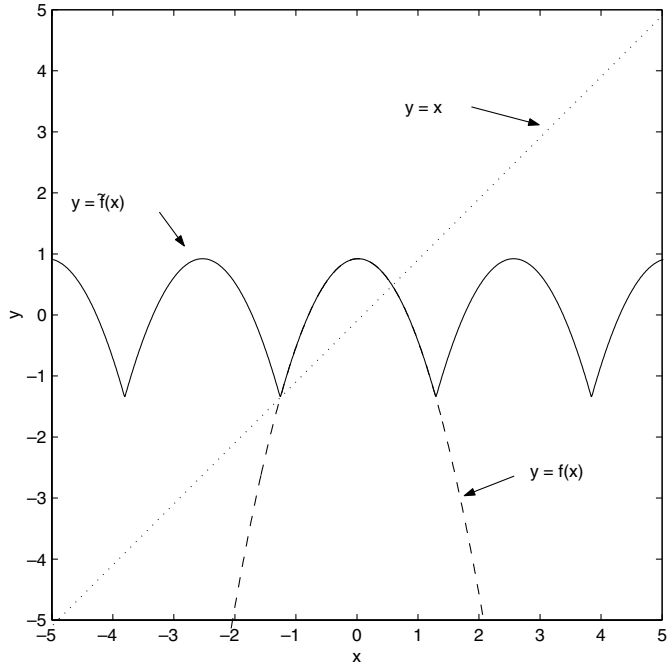

Fig. 4. Folding function proposed for Hénon's map modification.

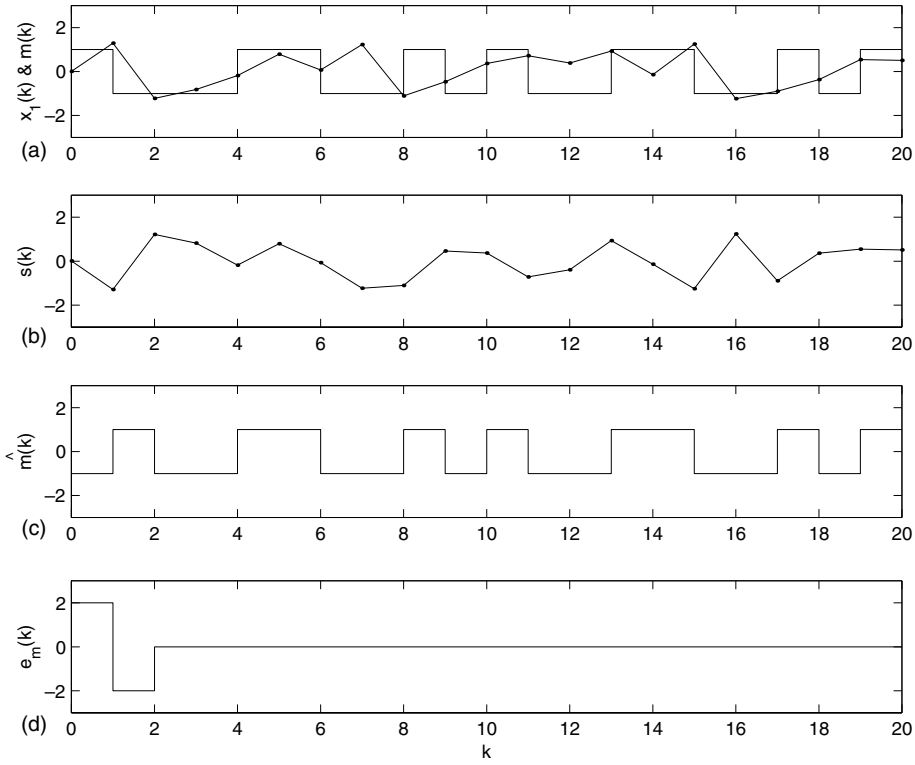

Fig. 5. Transmission using modulation by multiplication and feedback.

and chaotic behaviour is obtained for all initial conditions. Fig. 5 shows that the same message is now correctly transmitted while chaotic behaviour is preserved.

For more concrete application on digital communication of the modulation scheme using multiplication and feedback with the modified Hénon's map, Fig. 6 delineates an example of image transmission. The original image has been coded into a binary sequence, then modulated with a chaotic sequence and sent through a noiseless communication channel. It is shown that an intruder that has no knowledge about the chaotic modulating sequence can not extract the image, however it is shown that the image is correctly recovered at the appropriate receiver. The image has been next transmitted through a 30 dB AWGN channel, the recovered image is depicted in Fig. 6.

6. Conclusion

In this paper we have presented two chaotic modulation schemes for digital message transmission. By using the ability to synchronize discrete chaotic systems with the drive response concept, a digital binary message modulates the chaotic discrete sequence by simple multiplication. This scheme concerns a specified class of chaotic systems. To widen the class of chaotic systems concerned, the modulation procedure was altered by including a feedback loop to inject the transmitted signal to the transmitter. To recover the message an observer-based demodulator is used to synchronize with the transmitter system. This new scheme of chaotic communication can be applied to a large class of discrete chaotic systems. Moreover, some systems that may diverge due to the feedback loop can be slightly modified to satisfy the communication scheme requirements. A concrete example of message transmission is presented to illustrate the efficiency of our communication schemes.

It is worth noting that herein we have presented a single user communication scheme. However, our method can be extended to a multi-user scheme. In this case, the choice of the chaotic system that has adequate statistical properties is crucial to obtain feasible communication scheme. Work along these lines is in progress and the preliminary results are promising.

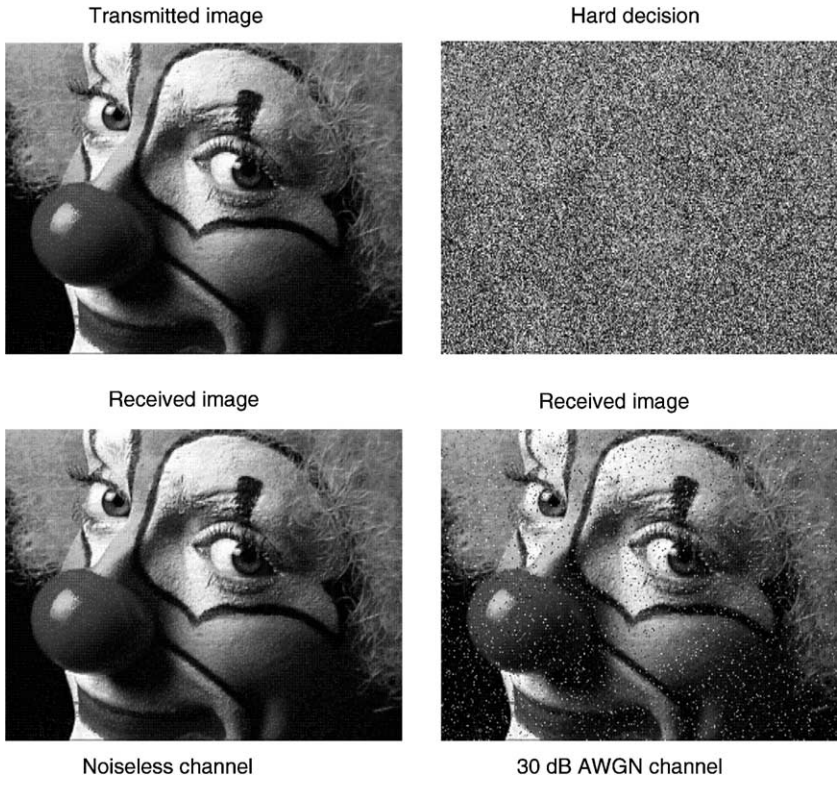

Fig. 6. Image transmission using the modified Hénon's map and chaotic modulation.

References

[1] Pecora LM, Carroll TL. Synchronization in chaotic systems. Physical Review Letters 1990;64(8):821–4.
[2] Morgül Ö, Feki M. On the synchronization of chaotic systems by using occasional coupling. Physical Review E 1997;55(5):5004–9.
[3] Pecora L, Carroll T, Johnson G, Mar D, Heagy J. Fundamentals of synchronization in chaotic systems, concepts, and applications. Chaos 1997;7(4):520–43.
[4] Huijberts H, Lilge T, Nijmeijer H. Nonlinear discrete-time synchronization via extended observers. International Journal of Bifurcation and Chaos 2001;11(7):1997–2006.
[5] Yang X-S, Chen G. Some observer-based criteria for discrete-time generalized chaos synchronization. Chaos, Solitons & Fractals 2002;13:1303–8.
[6] Feki M, Robert B. Observer-based chaotic synchronization in the presence of unknown inputs. Chaos, Solitons & Fractals 2003;15:831–40.
[7] Cuomo KM, Oppenheim AV, Strogatz SH. Synchronization of lorenzed-based chaotic circuits with applications to communications. IEEE Transactions on Circuits and Systems-II 1993;40(10):626–33.
[8] Morgül Ö, Feki M. A chaotic masking scheme by using synchronized chaotic systems. Physics Letters A 1999;251(3):169–76.
[9] Zhou C-S, Chen T-L. Robust communication via chaotic synchronization based on contraction maps. Physics Letters A 1997;225:60–6.
[10] Kennedy M, Kolumbán G. Digital communications using chaos. Signal Processing 2000;80:1307.
[11] Liao T-L, Huang N-S. Dead-beat chaos synchronization and its applications to image communications. IEICE Transactions on Fundamentals 1999;E82-A(8):1669–73.
[12] Dedieu H, Kennedy MP, Hasler M. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuit. IEEE Transactions on Circuits and Systems-II 1993;40(10):634–42.
[13] Itoh M, Murakami H. New communication systems via chaotic synchronizations and modulation. IEICE Transactions on Fundamentals 1995;E78-A(3):285–90.
[14] Kocarev U, Parlitz L. General approach for chaotic synchronization with applications to communication. Physical Review Letters 1995;74(25):5028–31.
[15] Andrievsky B. Adaptive synchronization methods for signal transmission on chaotic carrier. Mathematics and Computers in Simulation 2002;58:285–93.

[16] Cuomo KM, Oppenheim AV. Circuit implementation of synchronized chaos with applications to communications. Physical Review Letters 1993;71(1):65–8.
[17] Parlitz U, Ergezinger S. Robust communication based on chaotic spreading sequences. Physics Letters A 1994;188:146–50.
[18] Angeli A, Gebesio R, Tesi A. Dead-beat chaos synchronization in discrete-time systems. IEEE Transactions on Circuits and Systems-I 1995;42(1):54–6.
[19] Peitgen H, Jürgens H, Saupe D. Chaos and fractals: New frontiers of science. New York: Springer-Verlag; 1992.